UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/827,218	04/19/2004	Wael M. Ibrahim	200314912-1	2929

22879 7590 09/17/2009

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
3404 E. Harmony Road
Mail Stop 35
FORT COLLINS, CO 80528

EXAMINER	
REZA, MOHAMMAD W	
ART UNIT	PAPER NUMBER
2436	

NOTIFICATION DATE	DELIVERY MODE
09/17/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
ipa.mail@hp.com
jessica.l.fusek@hp.com

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/827,218
Filing Date: April 19, 2004
Appellant(s): IBRAHIM ET AL.

Peter Kraguljac (Reg. No. 38,520)

For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 06/11/2009 appealing from the Office action mailed 01/29/2009.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

This appeal involves claims 1-18, 45-48, and 48-49.

(4) Status of Amendments

The appellant's statement of the status of amendments rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct. However, the 35 USC 112 first, and second paragraphs rejections have been withdrawn regarding on claims 1-18, and 45-46, and 48-49.

(7) Claims Appendix

A copy of the appealed claims 1-18, 45-48, and 48-49 appears on pages in the Appendix to the appellant's brief is correct.

(8) Evidence Relied Upon

20030105965	David Carroll Challener
7,191,464	Cromer et al

(9) Grounds of Rejection

The 112 first, and second paragraphs rejections have been withdrawn regarding claims 1-18, and 45-46, and 48-49.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 1-18, 45-46, and 48-49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Challener (US patent app. pub. 20030105965) in view of Cromer et al hereafter Cromer (US Patent 7,191,464).

10. As per claim 1, Challener discloses a system, comprising: a logic configured to perform cryptographic key maintenance for a trusted platform to which the logic is bound (According to the figure 3 and paragraphs 0027, 0043, Challener teaches that the user's computer has the trusted platform module which is loaded with the piece of software (logic) to generate and migrate the cryptographic key to the credit card company (trusted platform) are connected together. Therefore, Challener teaches that the user's trusted platform module (TPM) loaded with software (logic) bound with the trusted platform (credit card company), where the cryptographic key maintenance

includes migrating a non-migratable storage root key from a root of a key storage hierarchy associated with a trusted platform module associated with the trusted platform a trusted platform to which the logic is bound in a one-to-one manner and an interface configured to facilitate operably connecting the system to the trusted platform (In fig. 2, customer creates the non-migratble key (element 202) and then provides (transfers or migrates) this non-migratble key to the credit card provider (the trusted platform), (element 205). In the same way, fig. 4 also shows that upon receiving the request form credit card company (the trusted platform, element 407), the end user sends (migrates) his non-migratble storage key to the credit card company (element 408), paragraphs, 0027-0033, 0043). Although, Challener discloses that a logic to perform cryptographic key maintenance for a trusted platform to which the logic is bound together. He does not expressly disclose the bound in a one-to-one manner with trusted platform. However, in the same field of endeavor, Cromer discloses the logic is bound to in a one-to-one manner with trusted platform (col. 4, lines 35-55, col. 3, lines 50-62).

Accordingly, it would been obvious to one of ordinary skill in the network security art at the time of invention was made to have incorporated Cromer's teachings of bound the logic with one-to-one manner with the teachings of Chanllener, for the purpose of suitably using the non-migratable key to be migrated in the trusted platform.

11. As per claim 2, Challener discloses the system where the cryptographic key maintenance performed by the logic comply with the Trusted Computing Group (TCG) specification version 1 .lb (paragraphs 0022-0024).

12. As per claim 3, Challener discloses the system where the logic comprises an application specific integrated circuit (ASIC) (abstract, paragraphs, 0007, 003-0031).

13. As per claim 4, Challener discloses the system where the logic comprises a microprocessor operably connected to a non-volatile memory (paragraphs, 0020).

14. As per claim 5, Challener discloses a system where a logic configured to perform one or more of key maintenance, and cryptographic key migration and an interface configured to facilitate operably connecting the system to the trusted platform and where the logic and the interface comprise part of a USB token (abstract, paragraphs, 0007, 003-0031). He does not expressly disclose the logic is bound to in a one-to-one manner with trusted platform. However, in the same field of endeavor, Cromer discloses the logic is bound to in a one-to-one manner with trusted platform (col. 4, lines 35-55, col. 3, lines 50-62).

The same motivation that was utilized in the combination of claim 1 applies equally as well to claim 5.

15. As per claim 6, Challener discloses the system where the logic is configured to migrate one or more nqn-miqratable keys from a trusted platform module associated with the trusted platform and configured to use the miglrated one or more non-migratable keys to decrypt items that were encrypted by the trusted platform module (abstract, paragraphs, 0007, 003-0031).

16. As per claim 7, Challener discloses the system where the logic is Configured to perform pofforming cryptographic key maintenance including cloning the trusted platform with the cooperation of a manufacturer of the trusted platform and an owner of

the trusted platform (paragraphs 0022-0024).

17. As per claim 8, Challener discloses the system where the to perform performing cryptographic key maintenance includes including having the manufacturer of the trusted platform act as an intermediary and migrating [[a]] the non-migratable storage root key from [[a]] the root of [[a]] the key storage hierarchy associated with [[a]] the trusted platform module associated with the trusted platform (abstract, paragraphs, 0007, 003-0031).

18. As per claim 9, Challener discloses the system where the logic is configured to performing cryptographic key migration including logically attaching a trusted platform module migratable key data structure associated with a first protected storage tree to a second protected storage tree (paragraphs, 0020).

19. As per claim 10, Challener discloses the system where the logic is configured to store one or more of, a copy of a storage root key, a binding data that facilitates binding the logic to the trusted platform in a one-to-one binding, a processor executable set of instructions that facilitate the trusted platform determining that the trusted platform is interfacing with the logic instead of [[a]] the trusted platform module, and a processor readable set of data that facilitates the trusted platform determining that the trusted platform is interfacing with the logic instead of a trusted platform module (paragraphs 0022-0024).

20. As per claim 11, Challener discloses the system where the logic is configured to facilitate substantially instantaneously restoring the trusted platform module (paragraphs, 0020).

21. As per claim 12, Challener discloses the system where the logic is configured to decrypt one or more of, a key, and a piece of data encrypted by [[a]] the trusted platform module (paragraphs, 0020).

22. As per claim 13, Challener discloses the system where the logic is configured to execute processor executable instructions associated with the logic while preventing execution of processor executable instructions not associated with the logic (abstract, paragraphs, 0007, 003-0031).

23. As per claim 14, Challener discloses the system where the logic is configured to read processor readable data associated with the logic while preventing a second logic from reading the processor readable data associated with the logic (paragraphs, 0020).

24. As per claim 15, Challener discloses the system where the logic is configured to detect whether there is a functional trusted platform module associated with the trusted platform (abstract, paragraphs, 0007, 003-0031).

25. As per claim 16, Challener discloses the system where the logic is configured to prevent creation of a new cryptographic key by the system and to prevent performance of an attestation service by the logic (paragraphs 0022-0024).

26. As per claim 17, Challener discloses the system where binding the logic to the trusted platform in a one-to-one manner includes producing an optimal asymmetric encryption padding (OEAP) binary large object to facilitate copying a storage root key stored in a trusted platform module associated with the trusted platform (paragraphs, 0020).

27. As per claim 18, Challener discloses the system the logic is configured to

perform a finite number of cryptographic key maintenance operations (abstract, paragraphs, 0007, 003-0031).

28. As per claim 45, Challener discloses a system, comprising: an electronic apparatus configured with a trusted platform module; and an interface operably connected to the electronic apparatus, and a subordinate trusted platform module to communicate with the trusted platform module via the interface, the subordinate trusted platform module including logic to migrate a non-migratable storage root key from the trusted platform module to be stored within the subordinate trusted platform module (abstract, paragraphs, 0007, 003-0031). He does not expressly discloses the interface configured to facilitate operably, detachably connecting a subordinate trusted platform module to the electronic apparatus. However, in the same field of endeavor, Cromer discloses the interface configured to facilitate operably, detachably connecting a subordinate trusted platform module to the electronic apparatus (col. 4, lines 35-55, col. 3, lines 50-62).

The same motivation that was utilized in the combination of claim 1 applies equally as well to claim 45.

29. As per claim 46, Challener discloses the system where the electronic apparatus comprises one of, a computer, a printer, a cellular telephone, and a digital camera (abstract, paragraphs, 0007, 003-0031).

30. As per claim 48, Challener discloses the system where the interface includes a port, and the subordinate trusted platform module is embodied in a removable

component that is attachable and detachable to the port (abstract, paragraphs, 0007, 003-0031).

31. As per claim 49, Challener discloses the system where the subordinate trusted platform module is configured to use the migrated non-migratable storage root key to decrypt items that were encrypted by the trusted platform module (abstract, paragraphs, 0007, 003-0031).

(10) Response to Argument

Regarding the 112 first paragraph, as failing to comply with the enablement requirement

Examiner withdraws the 112 first pagraph enablement requirement rejection regarding claims 1-18, and 45-46, and 48-49. As the appellant pointed in the specification of the present application how to render the present invention for any ordinary skill in the art without undue experiment. therefore examiner withdraws this rejection.

Regarding the 112 second paragraph, as failing to particularly point out and distinctly claim the subject matter

Examiner withdraws the 112 second pagraph rejection regarding claims 1-18, and 45-46, and 48-49. As appellant showed in the argument that the trusted platform module and trusted platform are two different platforms which clear the ambiguity of the claim limitation and therefore the 112 second paragraph rejection has been withdrawn.

Independent claim 1

Appellant argues that Challener does not disclose the claim element “migrating a non-migratable storage root key”. To establish this argument appellant wrongly cited the

portions of Challener from paragraph 0026. Actually, Challener mentions in this paragraph (0026) that this a current practice (Currently, a consumer expose his key… so, currently there is no requirement that keys be kept out of the hands of the consumer). However, that is not Challener's main invention. His invention is disclosed in the two alternative embodiments discussed in paragraphs, 0027-0033, and specifically, in paragraph, 0043. These paragraphs are also shown in figures 2 and 4 for migrating (transferring) the non-migratable storage key is from one place to another. In fig. 2, customer creates the non-migratble key (element 202) and then provides (transfers or migrates) this non-migratble key to the credit card provider (the trusted platform), (element 205). In the same way, fig. 4 also shows that upon receiving the request form credit card company (the trusted platform, element 407), the end user sends (migrates) his non-migratble storage key to the credit card company (element 408). Challener presents two alternative approaches against the current practice to generate the non-migtable storage key and transfers (migrates) this key form user associated with the trusted platform module (TPM) to credit card company (trusted platform). In paragraphs, 0027-0028, he discusses how to generate the non-migratble storage key and then the user decides if the non-migratable storage key requires any authorization from the credit card company. It is to be noted that the non-migratable storage key is generated by using the key function or software installed in the customer machine.

Additionally, regarding appellant's argument "Challener failure to teach "storage root key" as argued on page 14 par. 2, as recited in claim 1, argument is not persuasive because this storage key has been produced by using the stored grandparent, parent,

and child root key in a daisy chain fashioned (key storage hierarchy) inside the chip. Customer transfers (migrates) this non-migratable storage key to the credit card company for authorization (paragraph, 0030-00031). Further, Challener clearly teaches that the credit card company requests a secure non-migratable storage key form end user's trusted platform module which is associated with the end user's computer system. Then, the credit card company receives the secure non-migratable storage key from end user (paragraph, 0043). Therefore, it is apparent that requesting for the non-migrable storage key then receiving that key from the trusted platform module emphasis the teachings, "migrating a non-migratable storage key form one place to another." All these cited portions of Challener teach the claimed limitations.

Appellant also argues that the combined teaching of Challener and Cromer does not teach "logic is bound in a one-to-one manner". According to figure 1 and specification paragraph 003 of the present application, the subordinate trusted platform module includes a logic that may be configured to perform cryptographic key migration for trusted platform and they are bound together in a one-to-one manner. The same teachings have been found in Challener's invention as well. According to figure 3 and paragraphs 0027, 0043, Challener teaches that the user's computer has the trusted platform module which is loaded with the piece of software (logic) to generate and migrate the cryptographic key to the credit card company (trusted platform) are connected together. Therefore, Challener teaches that the user's trusted platform module (TPM) loaded with software (logic) bound with the trusted platform (credit card company) Further, Cromer teaches that TPM includes plurality of firmware of the

shadow PCRs(registers) linked one-to-one to the plurality of boot PCRs (col. 4, lines 35-38). Therefore any ordinary skill in the art would have been motivated to combine these two teachings to claim that the user's trusted platform module (TPM) loaded with software (logic) bound with the trusted platform (credit card company) in a one-to-one manner. As a result, it is shown that all the arguments presented by appellant have been traversed and the rejection should be sustained.

Independent claim 5

Appellant argues that the combined teachings of Challener do not teach "where the logic and the interface comprises part of a USB token". For the above mentioned discussion it is proved that Challener discloses the logic (software) installed inside the user device module (TPM) which performs the key migration. Further, in fig. 1, and paragraph, 0019 of Challener teaches that user interface connecting the system to the trusted platform and this interface which attached storage could be removable (USB capability). Therefore, Challener discloses the claimed limitations.

Dependent claim 6

In the above mentioned discussion it has been addressed why Challener teaches this claim limitation "the logic is configured to migrate one or more non-migratble keys".

Dependent claim 7

Appellant argues that Challener does not disclose, "where the logic is configured to perform cryptographic key maintenance including cloning the trusted platform with the cooperation of a manufacturer of the trusted platform and an owner of the trusted platform". Challener teaches the software or the key generating function (logic) which is

installed in the user system performs the cryptographic key generation and stores that key to the trusted platform (credit card company) (paragraphs, 0027-0028). Thus, it is disclosed the claimed limitation.

Dependent claim 17

Appellant argues that Challener fail to teach, "where binding the logic to the trusted platform in a one-to-one manner includes producing an optimal asymmetric encryption padding (OEAP) binary large object to facilitate copying a storage root key stored in a trusted platform module associated with the trusted platform". Examiner respectfully disagrees. Challener discloses that the logic (software) installed in the trusted platform module in the user device is binding to the trusted platform (credit card company) (figure 3 and paragraphs 0027, 0043). He also mentions that logic has been used to produce the encryption key which has been used to copy the storage root key in a trusted platform (paragraphs, 0027, 0043). Further, Cromer teaches that TPM includes the firmware of the plurality of shadow PCRS that are linked to the plurality of software of boot PCRs one-to-one manner (col. 4, lines 35-38). Therefore, the combined teachings of theses two inventions disclose the claim limitation.

Independent claim 45

Appellant further argues that Challener does not disclose "the interface configured to facilitate operably, detachably connecting a subordinate trusted platform module to the electronic apparatus." In fig. 1, and paragraph 0019, Challener mentions that user interface adapter facilitates the trusted platform module to connect to the electronic device and thus disclose the claim limitation.

(11) Related Proceedings Appendix

No decision rendered by a court of the Board is identified by the examiner in the Related Appeals and Interferences section of the examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Mohammad W Reza/

Examiner, Art Unit 2436

Conferees:

/Kimyen Vu/

Supervisory Patent Examiner, Art Unit 2435

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2436